Prob 1. Suppose nodes A and B are on the same 10 Mbps broadcast channel, and the propagation delay between the two nodes is 325 bit times. Suppose CSMA/CD and Ethernet packets are used for this broadcast channel. Suppose node A begins transmitting a frame and, before it finishes, node B begins transmitting a frame. Can A finish transmitting before it detects that B has transmitted? Why or why not? If the answer is yes, then A incorrectly believes that its frame was successfully transmitted without a collision. *Hint*: Suppose at time t=0 bits, A begins transmitting a frame. In the worst case, A transmits a minimum-sized frame of 512+64 bit times. So A would finish transmitting the frame at 512+64 bit times. Thus, the answer is no, if B's signal reaches A before bit time 512+64 bits. In the worst case, when does B's signal reach A?

Answer:

+) When t = 0, Node A begins transmitting a minimum-sized Ethernet frame. Then the total transmission time as d_trans, for a minimum frame (512 bits + 64-bit preamble) is:

=> t_finish = 512+ 64 = 576 bit time, then A finished transmitting

+) The worst case is, B begins transmitting at t = 324 bit time (assuming that the first bit of A's frame has not yet reached Node B. Node B senses the medium as idle and begins its transmission)

+) At t = 324+325=649 bit time, the first bit of Node B's signal finally reaches Node A. This's the earliest moment Node A can detect the collision.

+) Since t_detection > t_finish (649 > 576 bit time), Node A has already cleared its transmission buffer and moved to an "idle" or "success" state before the collision signal (interference) arrived at its interface.

Prob 2. Consider three LANs interconnected by two routers, as shown in **Figure 6.33** .

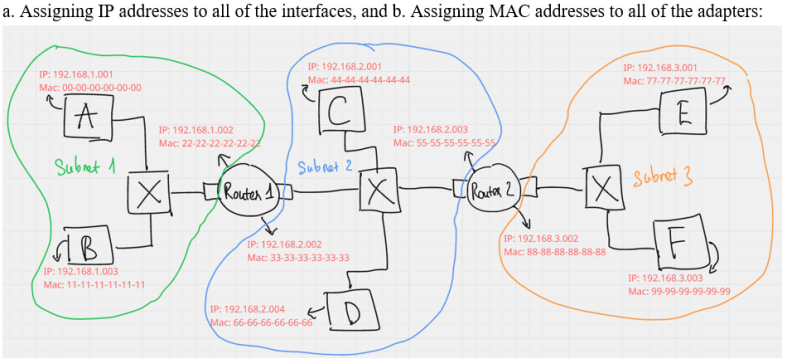
a. Assign IP addresses to all of the interfaces. For Subnet 1 use addresses of the form 192.168.1.xxx; for Subnet 2 uses addresses of the form 192.168.2.xxx; and for Subnet 3 use addresses of the form 192.168.3.xxx.

b. Assign MAC addresses to all of the adapters.

c. Consider sending an IP datagram from Host E to Host B. Suppose all of the ARP tables are up to date. Enumerate all the steps, as done for the single-router example in **Section 6.4.1** .

d. Repeat (c), now assuming that the ARP table in the sending host is empty (and the other tables are up to date).

a. Assigning IP addresses to all of the interfaces, and b. Assigning MAC addresses to all of the adapters:



c. Steps to send an IP datagram from host E to host B:

Step 1. Forwarding table in E determines that the datagram should be routed to interface 192.168.3.002.

Step 2. The adapter in E creates and Ethernet packet with Ethernet destination address 88-88-88-88-88-88.

Step 3. Router 2 receives the packet and extracts the datagram. The forwarding table in this router indicates that the datagram is to be routed to 198.162.2.002.

Step 4. Router 2 then sends the Ethernet packet with the destination address of 33-33-33-33-33-33 and source address of 55-55-55-55-55-55 via its interface with IP address of 198.162.2.003.

Step 5. The process continues until the packet has reached Host B.

d. Steps to send an IP datagram from host E to host B with an empty ARP table on host E:

Host E uses ARP to determine the MAC address of IP 198.162.3.2.

It sends an ARP request in a broadcast Ethernet frame.

Router 2 receives the request and replies with an ARP response, which is sent to Host E in an Ethernet frame with destination MAC address 77-77-77-77-77-77.

Prob 3. In this problem, you will put together much of what you have learned about Internet protocols. Suppose you walk into a room, connect to Ethernet, and want to download a Web page. What are all the protocol steps that take place, starting from powering on your PC to getting the Web page? Assume there is nothing in our DNS or browser caches when you power on your PC. (*Hint:* The steps include the use of Ethernet, DHCP, ARP, DNS, TCP, and HTTP protocols.) Explicitly indicate in your steps how you obtain the IP and MAC addresses of a gateway router.

Answer:

When I power on my computer and connect to Ethernet, the first thing that happens is the DHCP process. My computer sends out a DHCP Discover message, which is a special IP datagram addressed to 255.255.255.255. This datagram is placed inside an Ethernet frame and broadcast on the local network. The DHCP server responds with an Offer, and after the Request and Acknowledgment steps, my computer receives an IP address with a lease time. Along with the IP address, the DHCP server also provides the subnet mask, the IP address of the default gateway (first-hop router), and the IP address of a DNS server.

Since my ARP cache is empty at this point, my computer uses the ARP protocol to learn the MAC addresses of the gateway router and the DNS server. With this information, my computer can send frames directlv to these devices.

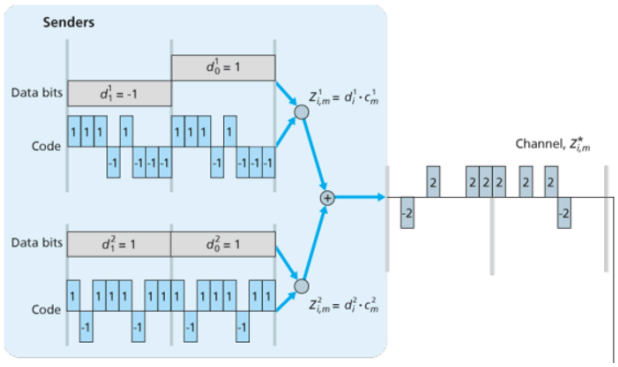
Next, when I want to download a web page, my computer needs the IP address of the web server hosting that page. It sends a DNS query to the local DNS server. If the DNS server does not already know the answer, it will perform recursive queries to resolve the domain name into an IP address and then return that IP address to my computer.

Once the IP address of the web server is known, my computer establishes a TCP connection with the server. This involves the three-way handshake (SYN, SYN-ACK, ACK). After the connection is set up, my computer sends an HTTP GET request for the web page. The HTTP request is encapsulated into TCP segments, which are then encapsulated into IP packets, and finally into Ethernet frames. These frames are sent to the gateway router, which forwards them based on its routing table. The packets are then routed across the Internet until they reach the destination web server.

The web server responds with HTTP response messages containing the requested page. These responses are encapsulated in TCP segments, IP packets, and Ethernet frames, and travel back through the Internet. When they reach my gateway router, the router forwards them to my computer. Finally, my computer reassembles the packets, processes the HTTP response, and displays the web page in my browser.

Prob 4. Suppose that the receiver in Figure 7.6 (in textbook) wanted to receive the data being sent sender 2. Show (by calculation) that the receiver is indeed able to recover sender 2's data from the aggregate channel signal by using sender 2's code.

Answer:



+) Sender 2's code (c^2) = [1, -1, 1, 1, 1, -1, 1, 1]

+) Number of chips (M) = 8

+) At time slot 1, the aggregate signal (Z*i, m) = [0, -2, 0, 2, 0, 0, 2, 2]

+) Using the formula

$$d_i^2 = \frac{\sum_{m=1}^{M} Z_{i,m}^* \cdot c_m^2}{M}$$

=> d^2_i = { 1*0 + (-1)*(-2) + 1*0 + 1*2 + 1*0 + (-1)*0 + 1*2 + 1*2 } / 8

=> d^2_i = 8/8 = 1

+) If my result is d^2_i = 1, then the decoded data bit for sender 2 is 1

Prob 6. What are the differences between the following types of wireless channel impairments: pathloss, multipath propagation, interference from other sources?

Answer:

1. Pathloss

- Definition: The reduction in the power density (attenuation) of an electromagnetic wave as it propagates through space.
- Primary Cause: Primarily the distance between the transmitter and the receiver. It is also affected by the frequency of the signal and environmental factors like atmospheric absorption or "shadowing" by large obstacles.
- Impact: It determines the maximum range of the communication link. If pathloss is too high, the signal-to-noise ratio (SNR) drops below the threshold required for successful decoding.

2. Multipath Propagation

- Definition: A phenomenon where the transmitted signal reaches the receiving antenna by two or more paths.
- Primary Cause: Reflection, diffraction, and scattering caused by physical objects in the environment (e.g., buildings, mountains, or indoor walls).
- Impact: This causes Fading (fluctuations in signal strength) and Inter-Symbol Interference (ISI). Since the "echoes" of the signal arrive at slightly different times, they can interfere with each other either constructively or destructively at the receiver.

3. Interference from Other Sources

- Definition: The disruption of the desired signal by other unwanted electromagnetic signals.
- Primary Cause: Other active transmitters operating on the same or adjacent frequency bands (e.g., a microwave oven or Bluetooth device interfering with a 2.4 GHz Wi-Fi signal).
- Impact: Unlike pathloss or multipath (which are properties of the channel/environment), interference is caused by external "noise." It decreases the SINR (Signal-to-Interference-plus-Noise Ratio), leading to higher bit error rates (BER) and reduced throughput.